

CLAIMS

1. A network system, comprising:
a first device to maintain an original resource;
a second device to maintain a replica resource remotely from the first device, the replica resource being replicated from the original resource;
memory to store a cached descriptor corresponding to the original resource;
a security component to determine whether the replica resource will pose a security risk to the second device upon receipt of a request for the replica resource, the security component:

formulating a descriptor corresponding to the replica resource and comparing the formulated descriptor with the cached descriptor; and

if the formulated descriptor and the cached descriptor are not equivalent, formulating a second descriptor corresponding to the original resource and comparing the formulated descriptor with the second descriptor.

2. A network system as recited in claim 1, wherein the security component determines that the replica resource is not a security risk if the formulated descriptor and the cached descriptor are equivalent.

3. A network system as recited in claim 1, wherein, if the formulated descriptor and the cached descriptor are not equivalent, and if the formulated descriptor and the second descriptor are equivalent, the security component determines that the replica resource is not a security risk.

1 4. A network system as recited in claim 1, wherein, if the formulated
2 descriptor and the cached descriptor are not equivalent, and if the formulated
3 descriptor and the second descriptor are equivalent, the security component
4 determines that the replica resource is not a security risk, and the cached descriptor
5 is replaced with the second descriptor.

6
7 5. A network system as recited in claim 1, wherein, if the formulated
8 descriptor and the cached descriptor are not equivalent, and if the formulated
9 descriptor and the second descriptor are not equivalent, the security component
10 determines that the replica resource is a security risk, and the replica resource is
11 replaced with a copy of the original resource.

12
13 6. A network system as recited in claim 1, wherein, if the formulated
14 descriptor and the cached descriptor are not equivalent, and if the formulated
15 descriptor and the second descriptor are not equivalent, the security component
16 determines that the replica resource is a security risk, the replica resource is
17 replaced with a copy of the original resource, and the cached descriptor is replaced
18 with the second descriptor.

19
20 7. A network system as recited in claim 1, wherein the security
21 component formulates the cached descriptor when the original resource is
22 replicated to create the replica resource.
23
24
25

1 8. A network system as recited in claim 1, wherein the security
2 component is configured to determine whether the request will pose a security risk
3 to the second device.
4

5 9. A network system as recited in claim 8, wherein the request
6 designates a resource locator.
7

8 10. A network system as recited in claim 8, wherein the request
9 designates a resource locator having a resource path, the resource path identifying
10 a location of the replica resource, and wherein the security component determines
11 that the request is not a security risk if the resource path does not exceed a
12 maximum number of characters.
13

14 11. A network system as recited in claim 8, wherein the request
15 designates a resource locator having a plurality of arguments, and wherein the
16 security component determines that the request is not a security risk if individual
17 arguments do not exceed a maximum number of characters, and if a total number
18 of characters defining all of the arguments do not exceed a maximum number of
19 characters.
20

21 12. A network system as recited in claim 8, wherein the request
22 designates a resource locator having a resource identifier, and wherein the security
23 component determines that the request is not a security risk if the resource
24 identifier has a valid file extension.
25

1 13. A network system as recited in claim 1, wherein:

2 the request designates a resource locator having a resource path and one or
3 more arguments, the resource path identifying a location of the replica resource
4 and the resource path having a resource identifier;

5 the security component is configured to determine whether the request will
6 pose a security risk to the second device;

7 the security component determines that the request is not a security risk if:

8 the resource path does not exceed a maximum number of characters;

9 individual arguments do not exceed a maximum number of
10 characters;

11 a total number of characters defining all of the arguments do not
12 exceed a maximum number of characters; and

13 the resource identifier has a valid file extension.

14
15 14. A network server, comprising:

16 a server component to receive a request for a resource maintained on the
17 network server and, in response to the request, implement security policies to
18 prevent unauthorized access to the resource; and

19 a security component that is registerable with the server component during
20 run-time to determine whether the request will pose a security risk to the network
21 server.

22
23 15. A network server as recited in claim 14, wherein, if the security
24 component determines that the request will pose a security risk, the security
25 component redirects the request to indicate that the resource is not available.

1
2 16. A network server as recited in claim 14, wherein the request
3 designates a resource locator having a resource path, the resource path identifying
4 a location of the resource, and wherein the security component determines that the
5 request is not a security risk if the resource path does not exceed a maximum
6 number of characters.

7
8 17. A network server as recited in claim 14, wherein the request
9 designates a resource locator having a plurality of arguments, and wherein the
10 security component determines that the request is not a security risk if individual
11 arguments do not exceed a maximum number of characters, and if a total number
12 of characters defining all of the arguments do not exceed a maximum number of
13 characters.

14
15 18. A network server as recited in claim 14, wherein the request
16 designates a resource locator having a resource identifier, and wherein the security
17 component determines that the request is not a security risk if the resource
18 identifier has a valid file extension.

19
20
21
22
23
24
25

1 **19.** A network server as recited in claim 14, wherein:
2 the request designates a resource locator having a resource path and one or
3 more arguments, the resource path identifying a location of the resource and the
4 resource path having a resource identifier;
5 the security component determines that the request is not a security risk if:
6 the resource path does not exceed a maximum number of characters;
7 individual arguments do not exceed a maximum number of
8 characters;
9 a total number of characters defining all of the arguments do not
10 exceed a maximum number of characters; and
11 the resource identifier has a valid file extension.

12
13 **20.** A network server, comprising:
14 a server component to receive a request for a resource maintained on the
15 network server and, in response to the request, implement security policies to
16 prevent unauthorized access to the resource; and
17 a security component that is registerable with the server component during
18 run-time to determine whether the resource will pose a security risk to the network
19 server upon receipt of the request.

20
21 **21.** A network server as recited in claim 20, wherein, if the security
22 component determines that the resource will pose a security risk, the security
23 component redirects the request to indicate that the resource is not available.
24
25

1 22. A network server as recited in claim 20, wherein the security
2 component:

3 formulates a descriptor corresponding to the resource;

4 compares the formulated descriptor with a cached descriptor, the cached
5 descriptor corresponding to the resource and formulated when the resource is
6 initially requested; and

7 determines that the resource is not a security risk if the formulated
8 descriptor and the cached descriptor are equivalent.

9
10 23. A network server as recited in claim 20, wherein the security
11 component:

12 formulates a descriptor corresponding to the resource;

13 compares the formulated descriptor with a cached descriptor, the cached
14 descriptor corresponding to the resource and formulated when the resource is
15 initially requested;

16 if the formulated descriptor and the cached descriptor are not equivalent,
17 formulates a second descriptor corresponding to an original resource maintained
18 on a file server remotely located from the network server, the resource being
19 replicated from the original resource;

20 compares the formulated descriptor with the second descriptor; and

21 determines that the resource is not a security risk if the formulated
22 descriptor and the second descriptor are equivalent.

1 **24.** A network server as recited in claim 20, wherein the security
2 component:

3 formulates a descriptor corresponding to the resource;

4 compares the formulated descriptor with a cached descriptor, the cached
5 descriptor corresponding to the resource and formulated when the resource is
6 initially requested;

7 if the formulated descriptor and the cached descriptor are not equivalent,
8 formulates a second descriptor corresponding to an original resource maintained
9 on a file server remotely located from the network server, the resource being
10 replicated from the original resource;

11 compares the formulated descriptor with the second descriptor;

12 if the formulated descriptor and the second descriptor are not equivalent,
13 initiates that the resource stored on the network server be replaced with a copy of
14 the original resource maintained on the file server; and

15 initiates that the cached descriptor be replaced with the second descriptor.
16

17 **25.** A network server, comprising:

18 an Internet server to receive a request for a resource maintained on the
19 network server and, in response to the request, implement security policies to
20 prevent unauthorized access to the resource;

21 a security component that is registerable with the Internet server during
22 run-time, the security component having:

23 a validation component to determine whether the request will pose a
24 security risk to the network server; and
25

1 an integrity verification component to determine whether the
2 resource will pose a security risk to the network server upon receipt of the
3 request.
4

5 26. A network server as recited in claim 25, wherein the request
6 designates a resource locator having a resource path, the resource path identifying
7 a location of the resource, and wherein the validation component determines that
8 the request is not a security risk if the resource path does not exceed a maximum
9 number of characters.
10

11 27. A network server as recited in claim 25, wherein the request
12 designates a resource locator having a plurality of arguments, and wherein the
13 validation component determines that the request is not a security risk if individual
14 arguments do not exceed a maximum number of characters, and if a total number
15 of characters defining all of the arguments do not exceed a maximum number of
16 characters.
17

18 28. A network server as recited in claim 25, wherein the request
19 designates a resource locator having a resource identifier, and wherein the
20 validation component determines that the request is not a security risk if the
21 resource identifier has a valid file extension.
22
23
24
25

1 29. A network server as recited in claim 25, wherein:

2 the request designates a resource locator having a resource path and one or
3 more arguments, the resource path identifying a location of the resource and the
4 resource path having a resource identifier;

5 the validation component determines that the request is not a security risk
6 if:

7 the resource path does not exceed a maximum number of characters;

8 individual arguments do not exceed a maximum number of
9 characters;

10 a total number of characters defining all of the arguments do not
11 exceed a maximum number of characters; and

12 the resource identifier has a valid file extension.

13
14 30. A network server as recited in claim 25, wherein the integrity
15 verification component:

16 formulates a descriptor corresponding to the resource;

17 compares the formulated descriptor with a cached descriptor, the cached
18 descriptor corresponding to the resource and formulated when the resource is
19 initially requested; and

20 determines that the resource is not a security risk if the formulated
21 descriptor and the cached descriptor are equivalent.
22
23
24
25

1 31. A network server as recited in claim 25, wherein the integrity
2 verification component:

3 formulates a descriptor corresponding to the resource;

4 compares the formulated descriptor with a cached descriptor, the cached
5 descriptor corresponding to the resource and formulated when the resource is
6 initially requested;

7 if the formulated descriptor and the cached descriptor are not equivalent,
8 formulates a second descriptor corresponding to an original resource maintained
9 on a file server remotely located from the network server, the resource being
10 replicated from the original resource;

11 compares the formulated descriptor with the second descriptor; and

12 determines that the resource is not a security risk if the formulated
13 descriptor and the second descriptor are equivalent.

14
15 32. A network server as recited in claim 25, wherein the integrity
16 verification component:

17 formulates a descriptor corresponding to the resource;

18 compares the formulated descriptor with a cached descriptor, the cached
19 descriptor corresponding to the resource and formulated when the resource is
20 initially requested;

21 if the formulated descriptor and the cached descriptor are not equivalent,
22 formulates a second descriptor corresponding to an original resource maintained
23 on a file server remotely located from the network server, the resource being
24 replicated from the original resource;

25 compares the formulated descriptor with the second descriptor;

1 if the formulated descriptor and the second descriptor are not equivalent,
2 initiates that the resource stored on the network server be replaced with a copy of
3 the original resource maintained on the file server; and

4 initiates that the cached descriptor be replaced with the second descriptor.

5
6 **33.** A computing device, comprising:
7 an operating system to access resources to service requests;
8 a security component to determine whether a resource will pose a security
9 risk to the computing device upon receipt of a request to access the resource;

10 the security component configured to:

11 formulate a descriptor corresponding to the resource;

12 retrieve a cached descriptor corresponding to the resource, the
13 cached descriptor stored on a remote second computing device;

14 compare the formulated descriptor with the cached descriptor; and

15 determine that the resource is not a security risk if the formulated
16 descriptor and the cached descriptor are equivalent.

17
18 **34.** A computing device as recited in claim 33, wherein the security
19 component formulates the cached descriptor when the resource is initially
20 requested.

21
22 **35.** A computing device as recited in claim 33, wherein the security
23 component initiates a remote data server to formulate the cached descriptor and
24 store the cached descriptor on the remote second computing device when the
25 resource is stored on the computing device.

1 36. A computing device as recited in claim 33, wherein, if the
2 formulated descriptor and the cached descriptor are not equivalent, the security
3 component initiates that the resource be replaced with a copy of the resource
4 maintained on the remote second computing device.
5

6 37. One or more computer readable media containing a security
7 application, comprising:

8 a validation component to determine whether a request for a resource poses
9 a security risk; and

10 an integrity verification component to determine whether the resource poses
11 a security risk.
12

13 38. Computer readable media as recited in claim 37, wherein the request
14 designates a resource locator having a resource path, the resource path identifying
15 a location of the resource, and wherein the validation component determines that
16 the request is not a security risk if the resource path does not exceed a maximum
17 number of characters.
18

19 39. Computer readable media as recited in claim 37, wherein the request
20 designates a resource locator having a plurality of arguments, and wherein the
21 validation component determines that the request is not a security risk if individual
22 arguments do not exceed a maximum number of characters, and if a total number
23 of characters defining all of the arguments do not exceed a maximum number of
24 characters.
25

1 **40.** Computer readable media as recited in claim 37, wherein the request
2 designates a resource locator having a resource identifier, and wherein the
3 validation component determines that the request is not a security risk if the
4 resource identifier has a valid file extension.

5
6 **41.** Computer readable media as recited in claim 37, wherein:
7 the request designates a resource locator having a resource path and one or
8 more arguments, the resource path identifying a location of the resource and the
9 resource path having a resource identifier;

10 the validation component determines that the request is not a security risk
11 if:

12 the resource path does not exceed a maximum number of characters;
13 individual arguments do not exceed a maximum number of
14 characters;

15 a total number of characters defining all of the arguments do not
16 exceed a maximum number of characters; and

17 the resource identifier has a valid file extension.

18
19 **42.** Computer readable media as recited in claim 37, wherein the
20 integrity verification component:

21 formulates a descriptor corresponding to the resource when the security
22 application receives the request;

23 compares the formulated descriptor with a cached descriptor, the cached
24 descriptor corresponding to the resource and formulated when the resource is
25 initially requested; and

1 determines that the resource is not a security risk if the formulated
2 descriptor and the cached descriptor are equivalent.

3
4 **43.** Computer readable media as recited in claim 37, wherein the
5 integrity verification component:

6 formulates a descriptor corresponding to the resource when the security
7 application receives the request;

8 compares the formulated descriptor with a cached descriptor, the cached
9 descriptor corresponding to the resource and formulated when the resource is
10 initially requested;

11 if the formulated descriptor and the cached descriptor are not equivalent,
12 formulates a second descriptor corresponding to an original resource remotely
13 located, the resource being replicated from the original resource;

14 compares the formulated descriptor with the second descriptor; and

15 determines that the resource is not a security risk if the formulated
16 descriptor and the second descriptor are equivalent.

17
18 **44.** Computer readable media as recited in claim 37, wherein the
19 integrity verification component:

20 formulates a descriptor corresponding to the resource when the security
21 application receives the request;

22 compares the formulated descriptor with a cached descriptor, the cached
23 descriptor corresponding to the resource and formulated when the resource is
24 initially requested;

1 if the formulated descriptor and the cached descriptor are not equivalent,
2 formulates a second descriptor corresponding to an original resource remotely
3 located, the resource being replicated from the original resource;

4 compares the formulated descriptor with the second descriptor;

5 if the formulated descriptor and the second descriptor are not equivalent,
6 initiates that the resource be replaced with a copy of the original resource; and

7 initiates that the cached descriptor be replaced with the second descriptor.

8
9 **45.** A method, comprising:

10 receiving a request for a replica resource stored on a computing device;

11 formulating a descriptor corresponding to the replica resource;

12 comparing the formulated descriptor with a cached descriptor
13 corresponding to an original resource stored on a second computing device
14 remotely located from the computing device, the replica resource being replicated
15 from the original resource;

16 determining that the replica resource does not pose a security risk if the
17 formulated descriptor and the cached descriptor are equivalent;

18 if the formulated descriptor and the cached descriptor are not equivalent,
19 formulating a second descriptor corresponding to the original resource;

20 comparing the formulated descriptor with the second descriptor; and

21 determining that the replica resource does not pose a security risk if the
22 formulated descriptor and the second descriptor are equivalent.

1 **46.** A method as recited in claim 45, further comprising allowing the
2 request if said determining that the replica resource does not pose a security risk to
3 the computing device.

4
5 **47.** A method as recited in claim 45, further comprising redirecting the
6 request to indicate that the replica resource is not available if determining that the
7 replica resource poses a security risk to the computing device.

8
9 **48.** A method as recited in claim 45, further comprising replacing the
10 cached descriptor with the second descriptor if the formulated descriptor and the
11 second descriptor are equivalent.

12
13 **49.** A method as recited in claim 45, further comprising replacing the
14 replica resource with a copy of the original resource if the formulated descriptor
15 and the cached descriptor are not equivalent, and if the formulated descriptor and
16 the second descriptor are not equivalent.

17
18 **50.** A method as recited in claim 45, further comprising replacing the
19 cached descriptor with the second descriptor if the formulated descriptor and the
20 cached descriptor are not equivalent, and if the formulated descriptor and the
21 second descriptor are not equivalent.

22
23 **51.** A method as recited in claim 45, further comprising formulating the
24 cached descriptor when the original resource is replicated to create the replica
25 resource.

1 **52.** A method as recited in claim 45, further comprising formulating the
2 cached descriptor when the replica resource is initially requested.

3
4 **53.** A method as recited in claim 45, further comprising determining
5 whether the request will pose a security risk.

6
7 **54.** A method as recited in claim 45, further comprising:
8 determining whether the request will pose a security risk; and
9 redirecting the request to indicate that the replica resource is not available if
10 determining that the request poses a security risk to the computing device.

11
12 **55.** A method as recited in claim 45, wherein the request designates a
13 resource locator having a resource path, the resource path identifying a location of
14 the replica resource, and the method further comprising determining that the
15 request does not pose a security risk if the resource path does not exceed a
16 maximum number of characters.

17
18 **56.** A method as recited in claim 45, wherein the request designates a
19 resource locator having a plurality of arguments, and the method further
20 comprising determining that the request does not pose a security risk if individual
21 arguments do not exceed a maximum number of characters, and if a total number
22 of characters defining all of the arguments do not exceed a maximum number of
23 characters.

1 57. A method as recited in claim 45, wherein the request designates a
2 resource locator having a resource identifier, and the method further comprising
3 determining that the request does not pose a security risk if the resource identifier
4 has a valid file extension.

5
6 58. A method as recited in claim 45, wherein:
7 the request designates a resource locator having a resource path and one or
8 more arguments, the resource path identifying a location of the replica resource
9 and the resource path having a resource identifier;
10 the method further comprising determining that the request does not pose a
11 security risk if:
12 the resource path does not exceed a maximum number of characters;
13 individual arguments do not exceed a maximum number of
14 characters;
15 a total number of characters defining all of the arguments do not
16 exceed a maximum number of characters; and
17 the resource identifier has a valid file extension.

18
19 59. A computer-readable medium comprising computer executable
20 instructions that, when executed, direct a computing system to perform the method
21 of claim 45.

22
23 60. A computer-readable medium comprising computer executable
24 instructions that, when executed, direct a computing system to perform the method
25 of claim 58.

1
2 **61.** A method, comprising:
3 receiving a request for a resource;
4 implementing security policies to prevent unauthorized access to the
5 resource;
6 determining whether the request will pose a security risk; and
7 determining whether the resource will pose a security risk if allowing the
8 request.

9
10 **62.** A method as recited in claim 61, further comprising allowing the
11 request for the resource if determining that the request does not pose a security
12 risk and if determining that the resource does not pose a security risk.

13
14 **63.** A method as recited in claim 61, wherein the request designates a
15 resource locator having a resource path, the resource path identifying a location of
16 the resource, and the method further comprising determining that the request does
17 not pose a security risk if the resource path does not exceed a maximum number of
18 characters.

19
20 **64.** A method as recited in claim 61, wherein the request designates a
21 resource locator having a plurality of arguments, and the method further
22 comprising determining that the request does not pose a security risk if individual
23 arguments do not exceed a maximum number of characters, and if a total number
24 of characters defining all of the arguments do not exceed a maximum number of
25 characters.

1
2 **65.** A method as recited in claim 61, wherein the request designates a
3 resource locator having a resource identifier, and the method further comprising
4 determining that the request does not pose a security risk if the resource identifier
5 has a valid file extension.

6
7 **66.** A method as recited in claim 61, further comprising:
8 formulating a descriptor corresponding to the resource;
9 comparing the formulated descriptor with a cached descriptor
10 corresponding to the resource and formulated when the resource is initially
11 requested; and
12 determining that the resource does not pose a security risk if the formulated
13 descriptor and the cached descriptor are equivalent.

14
15 **67.** A method as recited in claim 61, further comprising:
16 formulating a descriptor corresponding to the resource;
17 comparing the formulated descriptor with a cached descriptor
18 corresponding to the resource and formulated when the resource is initially
19 requested;
20 determining that the resource does not pose a security risk if the formulated
21 descriptor and the cached descriptor are equivalent;
22 if the formulated descriptor and the cached descriptor are not equivalent,
23 formulating a second descriptor corresponding to an original resource remotely
24 located, the resource replicated from the original source;
25 comparing the formulated descriptor with the second descriptor; and

1 determining that the resource does not pose a security risk if the formulated
2 descriptor and the second descriptor are equivalent.

3
4 **68.** A method as recited in claim 61, further comprising:
5 formulating a descriptor corresponding to the resource;
6 comparing the formulated descriptor with a cached descriptor
7 corresponding to the resource and formulated when the resource is initially
8 requested;

9 determining that the resource does not pose a security risk if the formulated
10 descriptor and the cached descriptor are equivalent;

11 if the formulated descriptor and the cached descriptor are not equivalent,
12 formulating a second descriptor corresponding to an original resource remotely
13 located, the resource replicated from the original resource;

14 comparing the formulated descriptor with the second descriptor; and

15 determining that the resource does not pose a security risk if the formulated
16 descriptor and the second descriptor are equivalent;

17 if the formulated descriptor and the second descriptor are not equivalent,
18 replacing the resource with a copy of the original resource and replacing the
19 cached descriptor with the second descriptor.

20
21 **69.** A computer-readable medium comprising computer executable
22 instructions that, when executed, direct a computing system to perform the method
23 of claim 61.
24
25

1 70. A computer-readable medium comprising computer executable
2 instructions that, when executed, direct a computing system to perform the method
3 of claim 68.

4
5 71. A method to determine whether an operating system can access a
6 resource without a security risk, the method comprising:

7 formulating a descriptor corresponding to the resource;
8 retrieving a cached descriptor corresponding to the resource, the cached
9 descriptor stored remotely;
10 comparing the formulated descriptor with the cached descriptor; and
11 determining that the resource is not a security risk if the formulated
12 descriptor and the cached descriptor are equivalent.

13
14 72. A method as recited in claim 71, further comprising allowing the
15 operating system to access the resource if said determining that the resource is not
16 a security risk.

17
18 73. A method as recited in claim 71, further comprising formulating the
19 cached descriptor when the resource is created.

20
21 74. A method as recited in claim 71, further comprising formulating the
22 cached descriptor when the resource is initially requested.
23
24
25

1 75. A computer-readable medium comprising computer executable
2 instructions that, when executed, direct a computing system to perform the method
3 of claim 71.
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25